

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-082043

(43)Date of publication of application : 21.03.2000

(51)Int.Cl.

G06F 15/00

(21)Application number : 10-252459

(71)Applicant : RICOH CO LTD

(22)Date of filing : 07.09.1998

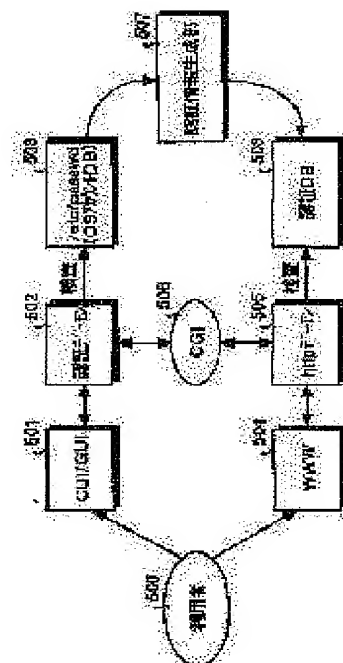
(72)Inventor : KAWAKAMI KAZUHIRO

(54) USER AUTHENTICATION SYSTEM, METHOD THEREFOR AND COMPUTER-READABLE RECORDING MEDIUM RECORDED WITH PROGRAM ALLOWING COMPUTER TO IMPLEMENT THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To easily, speedily, and securely perform user authentication by systems.

SOLUTION: This system is provided with an OS account DB 503 which stores OS account information including a log-in name and a password, an authentication demon 502 which authenticates a user by using the OS account information stored in the OS account DB 503, an authentication information generation part 507 which generates user authentication information according to the OS account information stored in the OS account DB 503, an authentication DB 508 generated by the authentication information generating means 507, and a http demon 505 which authenticates the user by using the user authentication information stored in the authentication DB 508.



LEGAL STATUS

[Date of request for examination]

05.11.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-82043

(P2000-82043A)

(43) 公開日 平成12年3月21日 (2000.3.21)

(51) Int.Cl.⁷

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

テーマコード(参考)

3 3 0 B 5 B 0 8 5

審査請求 未請求 請求項の数11 O L (全 16 頁)

(21) 出願番号

特願平10-252459

(22) 出願日

平成10年9月7日 (1998.9.7)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72) 発明者 川上 和博

東京都大田区中馬込1丁目3番6号 株式会社リコー内

(74) 代理人 100104190

弁理士 酒井 昭徳

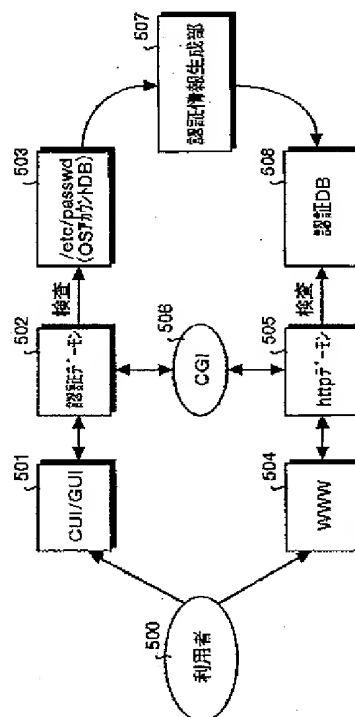
Fターム(参考) 5B085 AA08 AC03 AE01 BC01 BC07

(54) 【発明の名称】 利用者認証システム、利用者認証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 システムごとの利用者認証を容易、迅速、かつ確実におこなうことを課題とする。

【解決手段】 ログイン名およびパスワードを含むOSアカウント情報を格納するOSアカウントDB503と、OSアカウントDB503により格納されたOSアカウント情報を用いて利用者の認証をおこなう認証デーモン502と、OSアカウントDB503により格納されたOSアカウント情報に基づいて、利用者認証情報を生成する認証情報生成部507と、認証情報生成手段507により生成された認証DB508と、認証DB508により格納された利用者認証情報を用いて利用者の認証をおこなうhttpデーモン505とを備える。



【特許請求の範囲】

【請求項1】 ログイン名およびパスワードを含むOSアカウント情報を格納するOSアカウント情報格納手段と、

前記OSアカウント情報格納手段により格納されたOSアカウント情報を用いて利用者の認証をおこなう第1認証手段と、

前記OSアカウント情報格納手段により格納されたOSアカウント情報に基づいて、利用者認証情報を生成する生成手段と、

前記生成手段により生成された利用者認証情報を格納する利用者認証情報格納手段と、

前記利用者認証情報格納手段により格納された利用者認証情報を用いて利用者の認証をおこなう第2認証手段と、

を備えたことを特徴とする利用者認証システム。

【請求項2】 前記第1認証手段または前記第2の認証手段のいずれかを選択する選択手段を備え、前記選択手段により選択された認証手段により認証をおこなうことを特徴とする請求項1に記載の利用者認証システム。

【請求項3】 前記選択手段は、複数の認証手段が選択可能である場合、前記第1認証手段を選択することを特徴とする請求項2に記載の利用者認証システム。

【請求項4】 前記第1の認証手段および／または前記第2の認証手段は、

前記OSアカウント情報格納手段により格納されたOSアカウント情報または利用者認証情報格納手段により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことを特徴とする請求項1に記載の利用者認証システム。

【請求項5】 前記第1の認証手段および／または前記第2の認証手段は、

前記OSアカウント情報格納手段により格納されたOSアカウント情報を用いることができないとき、前記利用者認証情報格納手段により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうことを特徴とする請求項4に記載の利用者認証システム。

【請求項6】 ログイン名およびパスワードを含むOSアカウント情報を格納するOSアカウント情報格納工程と、

前記OSアカウント情報格納工程により格納されたOSアカウント情報を用いて利用者の認証をおこなう第1認証工程と、

前記OSアカウント情報格納工程により格納されたOSアカウント情報に基づいて、利用者認証情報を生成する生成工程と、

前記生成工程により生成された利用者認証情報を格納す

る利用者認証情報格納工程と、

前記利用者認証情報格納工程により格納された利用者認証情報を用いて利用者の認証をおこなう第2認証工程と、

を含んだことを特徴とする利用者認証方法。

【請求項7】 前記第1認証工程により認証をおこなうかまたは前記第2の認証工程により認証をおこなうかを選択する選択工程を含み、

前記選択工程により選択された認証工程により認証をおこなうことを特徴とする請求項6に記載の利用者認証方法。

【請求項8】 前記選択工程は、複数の認証工程により認証することが選択可能である場合、前記第1認証工程により認証するよう選択することを特徴とする請求項7に記載の利用者認証方法。

【請求項9】 前記第1認証工程および／または前記第2認証工程は、

前記OSアカウント情報格納工程により格納されたOSアカウント情報または利用者認証情報格納工程により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことを特徴とする請求項6に記載の利用者認証方法。

【請求項10】 前記第1認証工程および／または前記第2認証工程は、

前記OSアカウント情報格納工程により格納されたOSアカウント情報を用いることができないとき、前記利用者認証情報格納工程により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうことを特徴とする請求項9に記載の利用者認証方法。

【請求項11】 前記請求項6～10に記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、図書館情報管理システム等のシステムを利用する利用者の認証をおこなう利用者認証システム、利用者認証方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】従来の利用者認証システムについて図14を用いて説明する。図14において、1401は、利用者ID、ログイン名、パスワードの入力、認証結果の表示等をおこなうキャラクター・ユーザー・インターフェイス／グラフィカル・ユーザー・インターフェイス（CUI/GUI）であり、1402は、認証処理を司る制御部である認証デーモンであり、1403は、オペレーション・システム（OS）を利用する際のOSアカウント情報を格納する／etc/passwd（OSア

10

20

30

40

50

カウントDB)である。

【0003】また、1404は、ワールド・ワイド・ウェブ(WWW)であり、1405は、ハイパー・テキスト・トランスファー・プロトコル(http)デーモンであり、1406は、コモン・ゲートウェイ・インターフェイス(CGI)であり、1407はhttpパスワード・データベース(DB)である。

【0004】システム全体のOSを用いた或るシステム、たとえば、図書館情報管理システムを利用するための認証を要求する際、利用者1400は、CUI/GUI 1401に対して、ログイン名とパスワードを入力する。ログイン名とは、上記或るシステムを含むシステム全体のOS使用を使用する際、登録により与えられる個人のアカウント情報である。

【0005】CUI/GUI 1401は、ログイン名が入力された場合は、その入力されたログイン名をパスワードとともに認証デーモン1402へ渡す。認証デーモン1402は、/etc/passwd(OSアカウントDB) 1403に上記ログイン名およびパスワードを渡し、/etc/passwd(OSアカウントDB) 1403にあらかじめ登録されているログイン名およびパスワードと照合し、両者が一致するか否かを検査することにより認証の判定をおこなう。

【0006】一方、システム全体のOSを用いた或るシステムを利用するための認証を要求する際、利用者1400は、CUI/GUI 1401ではなく、WWW 1404に対して、ログイン名とパスワードを入力することもできる。

【0007】この場合、WWW 1404は、ログイン名が入力された場合は、その入力されたログイン名をパスワードとともにhttpデーモン1405へ渡す。httpデーモン1405は、httpパスワード・データベース(DB) 1407に上記ログイン名およびパスワードを渡し、httpパスワードDB 1407にあらかじめ登録されているログイン名およびパスワードと照合し、両者が一致するか否かを検査することにより認証の判定をおこなう。その後、httpデーモンは、CGI 1406を通じて、システム全体のOSとのデータの通信をおこなう。

【0008】このように、従来の利用者認証システムは、図書館情報管理システム等の或るシステムの利用をするための認証をする際、通常、システム全体のOSのアカウントDBを利用しておこなわれ、システム全体のOSのアカウント情報であるログイン名に対するパスワードが正しいかを検査し、正しい場合は、利用するシステムの許可を与えていた。

【0009】

【発明が解決しようとする課題】しかしながら、上記の従来技術にあつては、httpパスワードDB 1407に認証用ファイルを作成するおよび作成したファイルを

管理することはシステム管理者にとって煩雑であるとともに、httpパスワードDBをシステム全体のOSのOSアカウントDB 1403と同期をとることがきわめて困難であるため、確実に認証をおこなう際の障害になるという問題点があった。

【0010】また、混雑や故障等により、OSアカウントDB 1403により認証処理ができない状況になった場合に、システムの利用ができなくなるという問題点があった。

【0011】特に、図書閲覧システムを含む図書館情報管理システムの場合、図書館を利用する利用者数は膨大な数となるため、すべての利用者に対するログイン名をアカウントDBに登録し管理することを想定すると、この問題は顕著なものとなる。

【0012】この発明は、上述した従来例による問題点を解決するため、容易、迅速、かつ確実に利用者認証をおこなうことができる利用者認証システム、利用者認証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0013】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項1の発明に係る利用者認証システムは、ログイン名およびパスワードを含むOSアカウント情報を格納するOSアカウント情報格納手段と、前記OSアカウント情報格納手段により格納されたOSアカウント情報を用いて利用者の認証をおこなう第1認証手段と、前記OSアカウント情報格納手段により格納されたOSアカウント情報に基づいて、利用者認証情報を生成する生成手段と、前記生成手段により生成された利用者認証情報を格納する利用者認証情報格納手段と、前記利用者認証情報格納手段により格納された利用者認証情報を用いて利用者の認証をおこなう第2認証手段と、を備えたことを特徴とする。

【0014】また、請求項2の発明に係る利用者認証システムは、請求項1の発明において、前記第1認証手段または前記第2の認証手段のいずれかを選択する選択手段を備え、前記選択手段により選択された認証手段により認証をおこなうことを特徴とする。

【0015】また、請求項3の発明に係る利用者認証システムは、請求項2の発明において、前記選択手段が、複数の認証手段が選択可能である場合、前記第1認証手段を選択することを特徴とする。

【0016】また、請求項4の発明に係る利用者認証システムは、請求項1の発明において、前記第1の認証手段および/または前記第2の認証手段が、前記OSアカウント情報格納手段により格納されたOSアカウント情報または利用者認証情報格納手段により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことを特徴とする。

【0017】また、請求項5の発明に係る利用者認証システムは、請求項4の発明において、前記第1の認証手段および／または前記第2の認証手段が、前記OSアカウント情報格納手段により格納されたOSアカウント情報を用いることができないとき、前記利用者認証情報格納手段により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうことを特徴とする。

【0018】また、請求項6の発明に係る利用者認証方法は、ログイン名およびパスワードを含むOSアカウント情報を格納するOSアカウント情報格納工程と、前記OSアカウント情報格納工程により格納されたOSアカウント情報を用いて利用者の認証をおこなう第1認証工程と、前記OSアカウント情報格納工程より格納されたOSアカウント情報に基づいて、利用者認証情報を生成する生成工程と、前記生成工程により生成された利用者認証情報を格納する利用者認証情報格納工程と、前記利用者認証情報格納工程により格納された利用者認証情報を用いて利用者の認証をおこなう第2認証工程と、を含んだことを特徴とする。

【0019】また、請求項7の発明に係る利用者認証方法は、請求項6の発明において、前記第1認証工程により認証をおこなうかまたは前記第2の認証工程により認証をおこなうかを選択する選択工程を含み、前記選択工程により選択された認証工程により認証をおこなうことを特徴とする。

【0020】また、請求項8の発明に係る利用者認証方法は、請求項7の発明において、前記選択工程が、複数の認証工程により認証することが選択可能である場合、前記第1認証工程により認証するよう選択することを特徴とする。

【0021】また、請求項9の発明に係る利用者認証方法は、請求項6の発明において、前記第1認証工程および／または前記第2認証工程が、前記OSアカウント情報格納工程により格納されたOSアカウント情報または利用者認証情報格納工程により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことを特徴とする。

【0022】また、請求項10の発明に係る利用者認証方法は、請求項9の発明において、前記第1認証工程および／または前記第2認証工程が、前記OSアカウント情報格納工程により格納されたOSアカウント情報を用いることができないとき、前記利用者認証情報格納工程により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうことを特徴とする。

【0023】また、請求項11の発明に係る記憶媒体は、請求項6～10に記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムを機械読み取り可能となり、これによって、請求項6

～10の動作をコンピュータによって実現することが可能である。

【0024】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る利用者認証システム、利用者認証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【0025】（実施の形態1）まず、この発明の実施の形態1による利用者認証システムを含む図書館情報管理システム全体の構成を説明する。図1は、この発明の実施の形態1による利用者認証システムを含む図書館情報管理システム全体の構成を示す説明図である。図1において、図書館情報管理システムは、学術情報センター100と、図書館110と、サテライトライブラリ120と、事務室130と、計算機演習室140と、研究室150とがそれぞれ、専用回線あるいはインターネット等のネットワークで接続されている。

【0026】図書館110には、データ入力装置であるワークステーション（WS）111およびパーソナルコンピュータ（PC）112が、図書管理サーバー113および図書検索サーバー114に接続されている。その他、スキャナ115およびプリンタ116が同様にネットワークで接続されている。また、図書管理サーバー113は業務用データベース117を備えており、また、図書検索サーバー114は検索用データベース118を備えている。また、図書管理サーバー113および図書検索サーバー114をデータ入力装置とすることもできる。

【0027】また、サテライトライブラリ120、事務室130、計算機演習室140、研究室150には、データ入力装置であるWS121、141、151、あるいは、PC132、142、152がそれぞれ備えられている。

【0028】また、実施の形態1では、図書管理サーバー113と図書検索サーバー114とは別個の構成としたが、システム全体の規模等に応じて共用のサーバーとして運用するようにしてもよい。

【0029】図2は、実施の形態1による図書館情報管理システムの各サブシステムと図書館情報管理の業務との関係を示す説明図である。図2において、図書館情報管理システムは、目録管理を中心とした基本システム200と、図書検索システム201と、閲覧管理システム202と、発注受入システム203と、雑誌管理システム204と、蔵書点検システム205と、相互貸借システム206の6つのサブシステムから構成される。

【0030】基本システム200は、図書や雑誌の目録や所在を管理するためのシステムである。書誌データ、所蔵データの登録や修正、削除等をおこなうことにより、目録作成業務251を実行する。また、学術情報セ

ンター100が提供する目録システム(CAT)へ書誌情報を登録したり、学術情報センターに登録されている情報をローカルデータベースへ登録することにより、CATの利用業務252を実行する。さらに、図書館110内の図書の配架処理に関する配架業務253を実行する。

【0031】図書検索システム201は、図書館110内の端末(WS111、PC112)や、図書館110外の端末(WS121、141、151、PC132、142、152)から、図書や雑誌の書誌、所在、状態を検索・照合するためのシステムである。この図書館検索システム201には、たとえば、OPAC(Online Public Access Catalogue)が用いられる。

【0032】また、図書館検索システム201のインターフェイスには、キャラクター・ユーザー・インターフェイス(CUI)、グラフィカル・ユーザー・インターフェイス(GUI)、ワールド・ワイド・ウェブ(WWW)を用いることができ、これらにより、利用者による目録検索業務254を実行する。

【0033】閲覧管理システム202は、貸出返却や予約管理、延滞処理、利用者管理、利用統計等の閲覧に関する管理をするためのシステムである。これにより、貸出返却業務255、図書予約業務256、利用者管理業務257を実行する。

【0034】発注受入システム203は、購入依頼の受付から、重複チェック、予算チェック、発注受入、未納品チェックまで、図書(単行書)の発注受入をおこなうためのシステムである。これにより、購入調査業務258、発注業務259、受入業務260を実行する。

【0035】雑誌管理システム204は、図書館110で購入している雑誌や逐次刊行物の発注受入や契約管理、ならびに製本業務をおこなうためのシステムである。これにより、雑誌や逐次刊行物の購入調査業務258、発注業務259、受入業務260、さらには、製本業務261を実行する。

【0036】蔵書点検システム205は、図書館110が管理している図書資料の所在点検業務をおこなうためのシステムである。ハンディターミナル等を利用して、所在単位、書架単位で点検をおこなう。また、長期貸出者への所在調査票の出力もおこなう。これにより、蔵書点検業務262を実行する。

【0037】相互貸借システム206は、学術情報センター100の図書館間相互貸借(ILL)の受付・依頼情報をデータベースで管理するためのシステムである。文献複写や現物貸借に使用する各種の作業表の出力もおこなう。これにより、ILLによる貸借業務263を実行する。

【0038】つぎに、図書館情報管理システムのデータベースの構造について説明する。図3は、本実施の形態

による図書館情報管理システムのデータベースの構成を示す説明図である。図3において、図書館情報管理システムのデータベースは、業務用データベース117と、検索用データベース118と、さらに、サブシステム201~206間に共通のコード表310が格納されたコードマスターデータベース300とから構成される。

【0039】業務用データベース117は、主に図書館の職員が使うデータベースであり、図書館の職員が業務で作成、変更するデータは、すべて業務用データベース117に登録される。

【0040】業務用のデータベースには、購入依頼・発注受入データベース301と、雑誌管理データベース302と、目録(書誌、所蔵)データベース303と、所蔵点検・点検履歴データベース304と、貸出返却・貸出予約・利用者データベース305と、相互貸借・集計データベース306とを含む構造となっている。

【0041】購入依頼・発注受入データベース301は、発注受入システム203が利用するデータベースである。また、雑誌管理データベース302は、雑誌管理システム204が利用するシステムであり、雑誌管理とはたとえば雑誌の契約、発注、受入等である。また、目録(書誌、所蔵)データベース303は、発注受入システム203、雑誌管理システム204、目録管理システム200、蔵書点検システム205、閲覧管理システム202が利用するシステムである。

【0042】所蔵点検・点検履歴データベース304は、蔵書点検システム205が利用するシステムであり、貸出返却・貸出予約・利用者データベース305は、蔵書点検システム205、閲覧管理システム202が利用するシステムであり、相互貸借・集計データベース306は、相互貸借システム206が利用するシステムである。

【0043】また、検索用データベース118は、一般利用者が検索する際、参照するデータベースであり、図書雑誌検索データベース307が格納されている。検索するときに必要なのは、図書や雑誌の書誌と所蔵のデータであり、そのため、検索に必要なデータだけを業務用データベース117の中から取り出して、効率よく検索ができるデータの形式にして登録している。

【0044】つぎに、利用者認証システムを実現する図書管理サーバー113または図書検索サーバー114のハードウェア構成について説明する。図4は、実施の形態1による利用者認証システムのハードウェア構成を示すブロック図である。

【0045】図4において、401はシステム全体を制御するCPUを、402はブートプログラムを記憶したROMを、403はCPUのワークエリアとして使用されるRAMを、404はCPU401の制御にしたがってHD(ハードディスク)405に対するデータのリード/ライトを制御するHDD(ハードディスクドライ

10

20

30

40

50

ブ)を、405はHDD404の制御で書き込まれたデータを記憶するHDを、406はCPU401の制御にしたがってFD(フロッピーディスク)407に対するデータのリード/ライトを制御するFDD(フロッピーディスクドライブ)を、407はFDD406の制御で書き込まれたデータを記憶する着脱自在のFDを、408は文字、画像等を含むドキュメントや機能情報等を表示するディスプレイをそれぞれ示している。

【0046】また、409は通信回線410を介してネットワークNETに接続され、そのネットワークNETと内部のインターフェイスを司るインターフェイス(I/F)を、411は文字、数値、各種指示等の入力のためのキーを備えたキーボードを、412はカーソルの移動や範囲選択等をおこなうマウスを、413はOCR機能を含み、画像を光学的に読み取るスキャナを、414は、図書やカード等に付与(印刷)されたバーコードを読み取るバーコードリーダを、415はドキュメントやバーコード等を印刷するプリンタを、416は上記各部を接続するためのバスをそれぞれ示している。また、バス416は業務用データベース117にも接続されている。

【0047】また、図書検索サーバー114のハードウェア構成は、図書管理サーバー113のハードウェア構成とは、データベースが業務用データベース117であるか検索用データベース118であるかの違いをのぞき、その他はすべて同様であるので、その説明は省略する。さらに、本実施の形態では、図書管理サーバー113と図書検索サーバー114とは別個の構成としたが、システム全体の規模等に応じて共用のサーバーとして運用するようにしてもよい。

【0048】つぎに、実施の形態1による利用者認証システムの機能的な構成について説明する。図5は、実施の形態1による利用者認証システムの構成を示す機能ブロック図である。図5において、利用者認証システムは、キャラクター・ユーザー・インターフェイス(CUI)/グラフィカル・ユーザー・インターフェイス(GUI)501と、認証デーモン502と、/etc/passwd(OSアカウントデータベース(DB))503と、ワールド・ワイド・ウェブ(WWW)504と、ハイパー・テキスト・トランスファー・プロトコル(HTTP)デーモン505と、コモン・ゲートウェイ・インターフェイス(CGI)506と、認証情報生成部507と、認証データベース(DB)508とを含む構成となっている。

【0049】また、通常、ワールド・ワイド・ウェブ(WWW)504と、HTTPデーモン505と、コモン・ゲートウェイ・インターフェイス(CGI)506と、認証データベース(DB)508とにより、WWWサーバーが構成される。

【0050】CUI/GUI501は、認証を要求する

際、利用者がログイン名およびパスワードを入力するものである。また、CUI/GUI501は、認証結果を表示する。

【0051】認証デーモン502は、利用者認証処理を司る制御部であり、OSアカウントDB503により格納されたログイン名およびパスワードとCUI/GUI501により入力されたログイン名およびパスワードが一致するか否かを判断することにより利用者認証をおこなうものである。

【0052】/etc/passwd(OSアカウントデータベース(DB))503は、OSのアカウント情報であるログイン名およびパスワード等のOSのアカウント情報を格納する。

【0053】ワールド・ワイド・ウェブ(WWW)504は、インターネットで用いる情報検索システムの一つである。WWWブラウザ等を用いることにより、データの入力および表示をすることができる。

【0054】HTTPデーモン505は、HTTPによって利用者認証処理を含むデータ処理を司る制御部であり、CGI506とのデータの受渡しおよび認証DB508により格納されたアカウント情報とWWW504により入力されたアカウント情報とが一致するか否かを判断することにより利用者認証をおこなうものである。

【0055】コモン・ゲートウェイ・インターフェイス(CGI)506は、WWWサーバーから外部プログラムであるゲートウェイを呼び出して処理を依頼し、処理結果をWWW(ブラウザ)504に送信する。

【0056】認証情報生成部507は、OSアカウントDBに格納されている情報に基づいて、認証DB508に格納する認証情報を生成する。具体的には、システム運転停止時や利用者の少ない夜間に、OSアカウントDBからアカウント情報をコピーすることにより、WWWサーバー用である認証DBに格納する認証情報を生成する。また、認証データベース(DB)508は、認証情報生成部507により生成された認証情報を格納する。

【0057】利用者500は、2つの方法により利用者認証をおこなうことができる。一つの方法は、認証を要求する際、ログイン名およびパスワード等のアカウント情報をCUI/GUI501に入力する。CUI/GUI501は、入力されたログイン名およびパスワードを認証デーモン502に渡す。認証デーモン502は、通常、渡されたログイン名およびパスワードを、OSアカウントDB503へ渡して、OSアカウントDB503にあらかじめ登録されているログイン名およびパスワードと照合し、両者が一致するか否かを検査することにより認証の判定をおこなうものである。これは、従来のWWW504を使用しない場合の認証方法である。

【0058】一方、もう一つの方法は、認証を要求する際、ログイン名およびパスワード等のアカウント情報をWWW504に入力する。WWW504は、入力された

ログイン名およびパスワードをhttpデーモン505に渡す。httpデーモン505は、OSアカウントDB503とは別個に設けられた認証DB508を用いて、ログイン名およびパスワードの照合をおこない、両者が一致するか否かを検査することにより認証の判定をおこなうものである。これにより、CGI506および認証デーモン502を介してOSアカウントDBに依存することなく、利用者認証をおこなうことができる。

【0059】つぎに、利用者認証システムの認証情報生成部507による認証情報の生成処理の内容について説明する。図6は、実施の形態1による利用者認証システムの認証情報生成処理の手順を示すフローチャートである。

【0060】図6のフローチャートにおいて、まず、認証情報を生成する日時をあらかじめ設定する。日時としては、たとえば、毎日あるいは所定日数ごとの夜間の所定の時間としてもよく、また、システム運用を停止する日時等としてもよい。

【0061】そして、あらかじめ定められた所定日時となったか否かを判断する(ステップS601)。ここで、所定日時となるのを待って、所定日時となった場合(ステップS601肯定)は、つぎに、コピー元のOSアカウントDB503のアカウント情報の更新があったか否かを判断する(ステップS602)。ここで、更新がなかった場合(ステップS602否定)は、アカウント情報のコピーをする必要がないので、ステップS601へ移行し、再度、所定の日時になるのを待つ。

【0062】一方、ステップS602において、情報の更新があった場合(ステップS602肯定)は、認証情報の生成をおこなう(ステップS603)。具体的には、OSアカウントDB503の所定のアカウント情報をコピーすることによりおこなう。

【0063】つぎに、コピーされたアカウント情報を認証DB508に格納する(ステップS607)。これにより認証情報の生成処理は終了し、ステップS601へ移行し、再度、所定の日時になるのを待つ。

【0064】つぎに、実施の形態1による利用者認証システムの認証処理の内容について説明する。図7は、実施の形態1による利用者認証システムの認証処理の一連の手順を示すフローチャートである。

【0065】図7のフローチャートにおいて、まず、WWW504にログイン名が入力されたか否かを判断する(ステップS701)。ここで、ログイン名が入力されるのを待って、ログイン名が入力された場合(ステップS701肯定)は、つぎに、パスワードが入力されたか否かを判断する(ステップS702)。

【0066】ステップS702においても、ステップS701と同様に、パスワードが入力されるのを待って、パスワードが入力された場合(ステップS702肯定)は、ステップS701において入力されたログイン名と

ステップS702において入力されたパスワードをhttpデーモン505に渡す(ステップS703)。

【0067】ログイン名とパスワードを渡されたhttpデーモン505は、認証DB508を用いてログイン名およびパスワードの検査をおこなう(ステップS704)。検査の結果、ログイン名およびパスワードが認証DB508に格納されていたログイン名およびパスワードと一致するか否かを判断し(ステップS705)、不一致の場合(ステップS705否定)は、「NG(拒否)」を通知する(ステップS706)。その後、ステップS701へ移行し、再度のログイン名の入力进行。

【0068】ステップS705において、ログイン名およびパスワードが認証DB508にあらかじめ格納されていたログイン名およびパスワードと一致する場合(ステップS705肯定)は、「OK(承認)」を通知し(ステップS707)、その後、利用者500に対して、認証要求があったシステムを利用可能な状態にし(ステップS708)、すべての処理を終了する。

【0069】以上説明したように、実施の形態1によれば、認証情報生成部507により、OSアカウント情報と同期した内容のWWWサーバー用の認証情報を認証DB508内に生成するので、管理者に負担をかけることなく、システムのOSの認証と同様の認証をWWWサーバー側でおこなうことができる。

【0070】特に、複数のコンピュータシステムが任意の通信媒体を介して接続された分散環境において、特定のコンピュータシステムによって利用者情報を一元管理し、ログイン名およびパスワードにより利用者認証をおこない、分散環境上のサービスの利用を許可する利用者認証システムに対して有用である。

【0071】(実施の形態2)さて、実施の形態1では、CUI/GUIにより認証するか、WWWにより認証するかについては、認証をおこなう端末等によりあらかじめ定められていたが、以下に説明する実施の形態2のように、認証方式選択部により、いずれかの認証方式を選択できるようにしてもよい。

【0072】この発明の実施の形態2による利用者認証システムを含む図書館情報管理システム全体の構成、図書館情報管理システムの各サブシステムと図書館情報管理の業務との関係、図書館情報管理システムのデータベースの構造、および利用者認証システムを実現する図書管理サーバー113、図書検索サーバー114のハードウェア構成については、実施の形態1の図1～図4において説明した内容と同様であるので、その説明は省略する。

【0073】つぎに、実施の形態2による利用者認証システムの機能的な構成について説明する。図8は、実施の形態2による利用者認証システムの構成を示す機能ブロック図である。図8において、利用者認証システム

10

20

30

40

50

は、CUI/GUI801と、認証デーモン802と、OSアカウントDB803と、WWW804と、httpデーモン805と、CGI806と、認証情報生成部807と、認証DB808と、さらに、認証方式選択部810とを含む構成になっている。

【0074】CUI/GUI801、認証デーモン802、OSアカウントDB803、WWW804、httpデーモン805、CGI806、認証情報生成部807、認証DB808は、実施の形態1における図5のCUI/GUI501、認証デーモン502、OSアカウントDB503、WWW504、httpデーモン505、CGI506、認証情報生成部507、認証DB508と同様の構成であるので、その説明は省略する。

【0075】認証方式選択部810は、認証する際の2つの方式である、CUI/GUI801を用いるのか、あるいは、WWW804を用いるのかを選択することができる。選択の方法として、両方の認証方式を利用できることを前提として、いずれかの利用方式を利用者が選択するものである。これにより、利用者が所望する認証方式を選択することが可能である。

【0076】他の選択の方法として、あらかじめ認証方式に優先順位を付加しておき、その優先順位に基づいて、選択すべき認証方式を決定するものである。これにより、常に優先順位の高い認証方式が選択され、当該優先順位の高い認証方式による認証ができない場合に、つぎに優先順位の高い認証方式が選択されることにより、いずれかの認証方式に認証要求が集中しないようにすることができる。

【0077】つぎに、実施の形態2による利用者認証システムの認証処理の内容について説明する。図9は、実施の形態2による利用者認証システムの認証処理の一連の手順を示すフローチャートである。

【0078】図9のフローチャートにおいて、まず、利用者の認証する際、CUI/GUI801が選択されたか否かを判断する(ステップS901)。ここで、CUI/GUI801が選択されなかった場合(ステップS901否定)は、図7におけるステップS701へ移行し、WWW804による認証がおこなわれる。

【0079】一方、ステップS901において、CUI/GUI801が選択された場合(ステップS901肯定)は、つぎに、CUI/GUI801にログイン名が入力されたか否かを判断する(ステップS902)。ここで、ログイン名が入力されるのを待って、ログイン名が入力された場合(ステップS902肯定)は、つぎに、パスワードが入力されたか否かを判断する(ステップS903)。

【0080】ステップS903においても、ステップS902と同様に、パスワードが入力されるのを待って、パスワードが入力された場合(ステップS903肯定)は、ステップS902において入力されたログイン名と

ステップS902において入力されたパスワードを認証デーモン802へ渡す(ステップS904)。

【0081】ログイン名とパスワードを渡された認証デーモン802は、OSアカウントDB803を用いてログイン名およびパスワードの検査をおこなう(ステップS905)。検査の結果、ログイン名およびパスワードがOSアカウントDB803にあらかじめ格納されていたログイン名およびパスワードと一致するか否かを判断し(ステップS906)、不一致の場合(ステップS906否定)は、「NG(拒否)」を通知する(ステップS907)。その後、ステップS901へ移行し、再度、認証方式が選択されるのを待つ。

【0082】ステップS906において、ログイン名およびパスワードがOSアカウントDB803にあらかじめ格納されていたログイン名およびパスワードと一致する場合(ステップS906肯定)は、「OK(承認)」を通知し(ステップS908)、その後、利用者800に対して、認証要求があったシステムを利用可能な状態にし(ステップS909)、すべての処理を終了する。

【0083】つぎに、実施の形態2による利用者認証システムの認証方式選択部810の選択処理の一例について説明する。図10は、実施の形態2による利用者認証システムの認証方式選択部810の選択処理の手順を示すフローチャートである。

【0084】図10のフローチャートにおいて、まず、複数の認証方式が選択可能か否かを判断する(ステップS1001)。ここで、複数の認証方式の選択が可能な場合(ステップS1001肯定)は、あらかじめ定められた選択の優先順位に基づいて、たとえば、CUI/GUI801による認証方式を選択し、図9のステップS902へ移行する。

【0085】一方、ステップS1001において、複数の認証方式の選択が不可能でない場合(ステップS1001否定)は、つぎに、CUI/GUI801が選択可能であるか否かを判断する(ステップS1002)。ここで、CUI/GUI801が選択可能である場合(ステップS1002肯定)は、同じく図9のステップS902へ移行する。

【0086】一方、ステップS1002において、CUI/GUI801が選択可能でない場合(ステップS1002否定)は、つぎに、WWW804が選択可能であるか否かを判断する(ステップS1003)。ここで、WWW804が選択可能である場合(ステップS1003肯定)は、実施の形態1における図7のステップS701へ移行する。

【0087】一方、ステップS1003において、WWW804が選択可能でない場合(ステップS1003否定)は、選択できる認証方式が存在しないため、現状においては利用者認証ができない旨を警告し(ステップS1004)、選択処理を終了する。

10

20

30

40

50

【0088】以上説明したように、実施の形態2によれば、利用者が所望する認証方式を選択することができ、また、優先順位の高い認証方式による認証ができない場合に、つぎに優先順位の高い認証方式が選択されることにより、いずれかの認証方式に認証要求が集中しないようにし、効率的に認証処理をおこなうことができる。

【0089】また、複数の認証手段が選択可能な場合には、OSアカウントDB803のアカウント情報を用いて認証処理をおこなうため、認証処理をより迅速におこなうことができる。

【0090】特に、複数のコンピュータシステムが任意の通信媒体を介して接続された分散環境において、特定のコンピュータシステムによって利用者情報を一元管理し、利用者IDおよびパスワードにより利用者認証をおこない、分散環境上のサービスの利用を許可する利用者認証システムに対して有用である。

【0091】（実施の形態3）さて、実施の形態1および2では、認証デーモンはOSアカウントDBを用いて認証をおこない、httpデーモンは認証DBを用いて認証をおこなっていたが、以下に説明する実施の形態3のように、認証デーモンがOSアカウントDBまたは認証DBを選択的に用いることにより、認証処理をおこなうようにしてもよい。

【0092】この発明の実施の形態3による利用者認証システムを含む図書館情報管理システム全体の構成、図書館情報管理システムの各サブシステムと図書館情報管理の業務との関係、図書館情報管理システムのデータベースの構造、および利用者認証システムを実現する図書管理サーバー113、図書検索サーバー114のハードウェア構成については、実施の形態1の図1～図4において説明した内容と同様であるので、その説明は省略する。

【0093】つぎに、実施の形態3による利用者認証システムの機能的な構成について説明する。図11は、実施の形態2による利用者認証システムの構成を示す機能ブロック図である。図11において、利用者認証システムは、CUI/GUI1101と、認証デーモン1102と、OSアカウントDB1103と、WWW1104と、httpデーモン1105と、CGI1106と、認証情報生成部1107と、認証DB1108を含む構成となっている。

【0094】ここで、認証デーモン1102をのぞく、CUI/GUI1101、OSアカウントDB1103、WWW1104、httpデーモン1105、CGI1106、認証情報生成部1107、認証DB1108は、実施の形態1における図5のCUI/GUI701、OSアカウントDB703、WWW704、httpデーモン705、CGI706、認証情報生成部707、認証DB708と同様の構成であるので、その説明

は省略する。

【0095】認証デーモン1102は、利用者認証処理を司る制御部であり、OSアカウントDB1103により格納されたログイン名およびパスワードとCUI/GUI1101により入力されたログイン名およびパスワードが一致するか否かを判断することにより利用者認証をおこなうものである。

【0096】また、認証デーモン1102は、認証DB1108により格納されたログイン名およびパスワードとCUI/GUI1101により入力されたログイン名およびパスワードが一致するか否かを判断することにより利用者認証をおこなうこともできる。したがって、認証デーモン1102は、OSアカウントDB1103と認証DB1108を選択的に用いることができる。これにより、OSアカウントDB1103が使用不可能な状態となった場合等に、認証DB1108を用いて、迅速に認証をすることができる。

【0097】OSアカウントDB1103または認証DB1108のいずれかを選択する方法としては、優先順位をあらかじめ設定し、優先順位の高いDBを選択する。ここで、優先順位の高いDBが利用可能な状態でない場合は、つぎに優先順位の高いDBを選択する。また、利用者1100に所望のDBを選択させる方法や、乱数を発生させ、認証する都度、発生させた乱数に基づいてランダムにDBを選択する方法であってもよい。

【0098】利用者1100は、認証を要求する際、ログイン名およびパスワードをCUI/GUI1101に入力する。CUI/GUI1101は、入力されたログイン名およびパスワードを認証デーモン1102に渡す。認証デーモン1102は、DBを選択し、選択したDBへログイン名およびパスワードを渡して、上記DBにあらかじめ登録されているログイン名およびパスワードと照合し、両者が一致するか否かを検査することにより認証の判定をおこなう。

【0099】つぎに、実施の形態3による利用者認証システムの認証処理の内容について説明する。図12は、実施の形態3による利用者認証システムの認証処理の手順を示すフローチャートである。

【0100】図12のフローチャートにおいて、まず、CUI/GUI1101にログイン名が入力されたか否かを判断する（ステップS1201）。ここで、ログイン名が入力されるのを待って、ログイン名が入力された場合（ステップS1201肯定）は、つぎに、パスワードが入力されたか否かを判断する（ステップS1202）。

【0101】ステップS1202においても、ステップS1201と同様に、パスワードが入力されるのを待って、パスワードが入力された場合（ステップS1202肯定）は、ステップS1201において入力されたログイン名とステップS1202において入力されたパスワ

ードを認証デーモン1102へ渡す(ステップS1203)。

【0102】つぎに、OSアカウントDB1103が選択されたか否かを判断する(ステップS1204)。ここで、OSアカウントDB1103が選択された場合(ステップS1204肯定)は、実施の形態2による図9のステップS905へ移行する。

【0103】一方、ステップS1204において、OSアカウントDB1103が選択されなかった場合(ステップS1204否定)は、認証DB1108を用いてログイン名およびパスワードの検査をおこなう(ステップS1205)。検査の結果、ログイン名およびパスワードが認証DB1108にあらかじめ格納されていたログイン名およびパスワードと一致するか否かを判断し(ステップS1206)、不一致の場合(ステップS1206否定)は、「NG(拒否)」を通知する(ステップS1207)。その後、ステップS1201へ移行し、再度のログイン名の入力を待つ。

【0104】ステップS1206において、ログイン名およびパスワードが上記選択されたDBにあらかじめ格納されていたログイン名およびパスワードと一致する場合(ステップS1206肯定)は、「OK(承認)」を通知し(ステップS1208)、その後、利用者1100に対して、認証要求があったシステムを利用可能な状態にし(ステップS1209)、すべての処理を終了する。

【0105】つぎに、実施の形態3による利用者認証システムの認証デーモン1102のDB選択処理の一例について説明する。図13は、実施の形態3による利用者認証システムの利用者認証処理の別の手順を示すフローチャートである。

【0106】図13のフローチャートにおいて、ステップS1301～S1303は、図12のステップS1201～S1203と同様の内容なので、それらの説明は省略する。

【0107】ステップS1303において、ステップS1301において入力されたログイン名とステップS1302において入力されたパスワードを認証デーモン1102へ渡した後、OSアカウントDB1103のOSアカウント情報が利用可能か否かを判断する(ステップS1304)。ここで、OSアカウント情報が利用可能な場合(ステップS1304肯定)は、実施の形態2による図9のステップS905へ移行する。

【0108】一方、ステップS1304において、OSアカウント情報が利用可能でない場合(ステップS1304否定)は、つぎに、認証DB1108を用いてログイン名およびパスワードの検査をおこなう(ステップS1305)。以下、ステップS1305～S1309は、図12のステップS1205～S1209と同様の内容なので、それらの説明は省略する。

【0109】以上説明したように、実施の形態3によれば、複数のDBから一つのDBを選択し、選択されたDBを用いて認証処理をおこなうので、複数のDBを選択的に用いるので、DBの稼働率を向上させ、効率よく認証処理をすることができる。また、いずれかのDBが利用できない場合であっても、利用できるDBを用いて認証処理を確実にこなうことができる。

【0110】特に、複数のコンピュータシステムが任意の通信媒体を介して接続された分散環境において、特定のコンピュータシステムによって利用者情報を一元管理し、ログイン名およびパスワードにより利用者認証をおこない、分散環境上のサービスの利用を許可する利用者認証システムに対して有用である。

【0111】なお、実施の形態1から3で説明した利用者認証方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーション等のコンピュータで実行することにより実現される。このプログラムは、ハードディスク、フロッピーディスク、CD-ROM、MO、DVD等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。またこのプログラムは、上記記録媒体を介してまたはネットワークを介して配布することができる。

【0112】

【発明の効果】以上説明したように、請求項1の発明によれば、ログイン名およびパスワードを含むOSアカウント情報を格納するOSアカウント情報格納手段と、前記OSアカウント情報格納手段により格納されたOSアカウント情報を用いて利用者の認証をおこなう第1認証手段と、前記OSアカウント情報格納手段により格納されたOSアカウント情報に基づいて、利用者認証情報を生成する生成手段と、前記生成手段により生成された利用者認証情報を格納する利用者認証情報格納手段と、前記利用者認証情報格納手段により格納された利用者認証情報を用いて利用者の認証をおこなう第2認証手段と、を備えているため、管理者に負担をかけることなく、システムのOSの認証と同様の認証をWWWサーバー側でおこなうことができ、容易かつ確実に利用者認証をおこなうことができる利用者認証システムが得られるという効果を奏する。

【0113】また、請求項2の発明によれば、請求項1の発明において、前記第1認証手段または前記第2の認証手段のいずれかを選択する選択手段を備え、前記選択手段により選択された認証手段により認証をおこなうため、利用者が所望する認証方式を選択することができ、また、優先順位の高い認証方式による認証ができない場合に、つぎに優先順位の高い認証方式が選択されることにより、いずれかの認証方式に認証要求が集中しないようにし、効率的に認証処理をおこなうことができ、迅速かつ確実に利用者認証をおこなうことができる利用者認

証システムが得られるという効果を奏する。

【0114】また、請求項3の発明によれば、請求項2の発明において、前記選択手段が、複数の認証手段が選択可能である場合、前記第1認証手段を選択するため、迅速かつ確実に利用者認証をおこなうことができる利用者認証システムが得られるという効果を奏する。

【0115】また、請求項4の発明によれば、請求項1の発明において、前記第1の認証手段および／または前記第2の認証手段が、前記OSアカウント情報格納手段により格納されたOSアカウント情報または利用者認証情報格納手段により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうため、複数のDBから一つのDBを選択し、選択されたDBを用いて認証処理をおこなうので、複数のDBを選択的に用いるので、DBの稼働率を向上させ、効率よく認証処理をすることができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証システムが得られるという効果を奏する。ことを特徴とする。

【0116】また、請求項5の発明によれば、請求項4の発明において、前記第1の認証手段および／または前記第2の認証手段が、前記OSアカウント情報格納手段により格納されたOSアカウント情報を用いることができないとき、前記利用者認証情報格納手段により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうため、いずれかのDBが利用できない場合であっても、利用できるDBを用いて認証処理をおこなうことができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証システムが得られるという効果を奏する。

【0117】また、請求項6の発明によれば、ログイン名およびパスワードを含むOSアカウント情報を格納するOSアカウント情報格納工程と、前記OSアカウント情報格納工程により格納されたOSアカウント情報を用いて利用者の認証をおこなう第1認証工程と、前記OSアカウント情報格納工程により格納されたOSアカウント情報に基づいて、利用者認証情報を生成する生成工程と、前記生成工程により生成された利用者認証情報を格納する利用者認証情報格納工程と、前記利用者認証情報格納工程により格納された利用者認証情報を用いて利用者の認証をおこなう第2認証工程と、を含んでいるため、管理者に負担をかけることなく、システムのOSの認証と同様の認証をWWWサーバー側でおこなうことができ、容易かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【0118】また、請求項7の発明によれば、請求項6の発明において、前記第1認証工程により認証をおこなうかまたは前記第2の認証工程により認証をおこなうかを選択する選択工程を含み、前記選択工程により選択された認証工程により認証をおこなうことため、利用者が所望する認証方式を選択することができ、また、優先順

位の高い認証方式による認証ができない場合に、つぎに優先順位の高い認証工程が選択されることにより、いずれかの認証工程に認証要求が集中しないようにし、効率的に認証処理をおこなうことができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【0119】また、請求項8の発明によれば、請求項7の発明において、前記選択工程は、複数の認証工程により認証することが選択可能である場合、前記第1認証工程により認証するよう選択するため、迅速かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【0120】また、請求項9の発明によれば、請求項6の発明において、前記第1認証工程および／または前記第2認証工程が、前記OSアカウント情報格納工程により格納されたOSアカウント情報または利用者認証情報格納工程により格納された利用者認証情報のいずれかを選択し、選択された情報を用いて利用者の認証をおこなうことため、各工程における処理の稼働率を向上させ、効率よく認証処理をすることができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【0121】また、請求項10の発明によれば、請求項9の発明において、前記第1認証工程および／または前記第2認証工程は、前記OSアカウント情報格納工程により格納されたOSアカウント情報を用いることができないとき、前記利用者認証情報格納工程により格納された利用者認証情報を選択し、前記利用者認証情報を用いて利用者の認証をおこなうため、いずれかの工程による処理をおこなうことができない場合であっても、利用できる工程により認証処理をおこなうことができ、迅速かつ確実に利用者認証をおこなうことができる利用者認証方法が得られるという効果を奏する。

【0122】また、請求項11の発明に係る記憶媒体は、請求項6～10に記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムを機械読み取り可能となり、これによって、請求項6～10の動作をコンピュータによって実現することが可能な記録媒体が得られるという効果を奏する。

【図面の簡単な説明】

【図1】この発明の実施の形態1による図書館情報管理システム全体の構成を示す説明図である。

【図2】実施の形態1による図書館情報管理システムの各サブシステムと図書館情報管理の業務との関係を示す説明図である。

【図3】実施の形態1による図書館情報管理システムのデータベースの構成を示す説明図である。

【図4】実施の形態1による図書館情報管理システムの図書管理サーバーのハードウェア構成を示すブロック図である。

【図 5】実施の形態 1 による利用者認証システムの構成を示す機能ブロック図である。

【図 6】実施の形態 1 による利用者認証システムの認証情報生成処理の手順を示すフローチャートである。

【図 7】実施の形態 1 による利用者認証システムの認証処理の手順を示すフローチャートである。

【図 8】この発明の実施の形態 2 による利用者認証システムの構成を示す機能ブロック図である。

【図 9】実施の形態 2 による利用者認証システムの認証処理の手順を示すフローチャートである。

【図 10】実施の形態 2 による利用者認証システムの認証方式選択部の選択処理の手順を示すフローチャートである。

【図 11】この発明の実施の形態 3 による利用者認証システムの構成を示す機能ブロック図である。

【図 12】実施の形態 3 による利用者認証システムの認証処理の手順を示すフローチャートである。

【図 13】実施の形態 3 による利用者認証システムの利用者認証処理の別の手順を示すフローチャートである。

【図 14】従来の利用者認証システムの構成を示す機能ブロック図である。

【符号の説明】

100 学術情報センター

110 図書館

111, 121, 141, 151 ワークステーション (WS)

112, 132, 142, 152 パーソナルコンピュータ (PC)

113 図書管理サーバー

114 図書検索サーバー

117 業務用データベース

118 検索用データベース

120 サテライブラリ

130 事務室

140 計算機演習室

150 研究室

200 基本 (目録管理) システム

201 図書検索システム

202 閲覧システム

203 発注受入システム

204 雑誌管理システム

10 205 蔵書点検システム

401 CPU

405 HD

407 FD

408 ディスプレイ

409 インターフェイス (I/F)

410 通信回線

411 キーボード

412 マウス

413 スキャナ

414 バーコードリーダー

500, 800, 1100 利用者

501, 801, 1101 CUI/GUI

502, 802, 1102 認証デーモン

503, 803, 1103 /etc/passwd
(OSアカウントDB)

504, 804, 1104 WWW

505, 805, 1105 httpデーモン

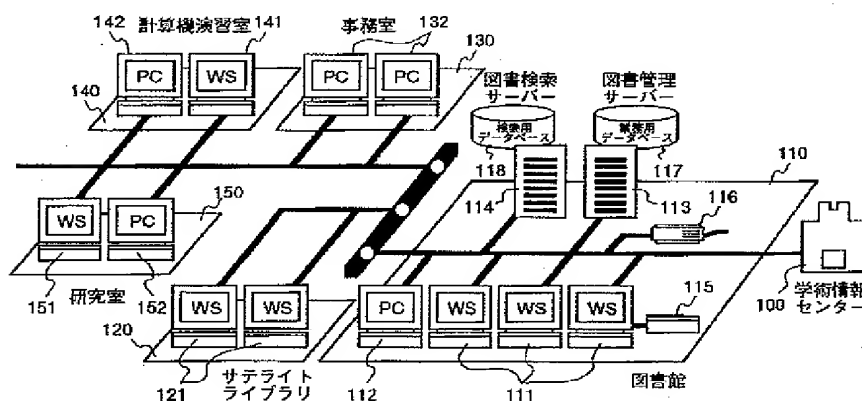
506, 806, 1106 CGI

507, 807, 1107 認証情報生成部

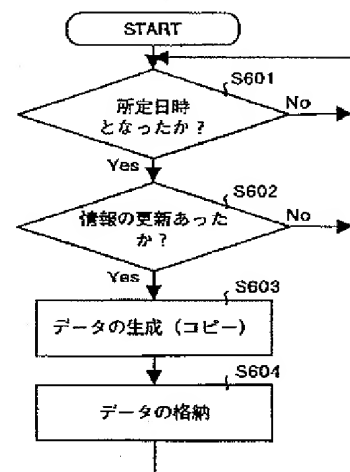
30 508, 808, 1108 認証DB

810 認証方式選択部

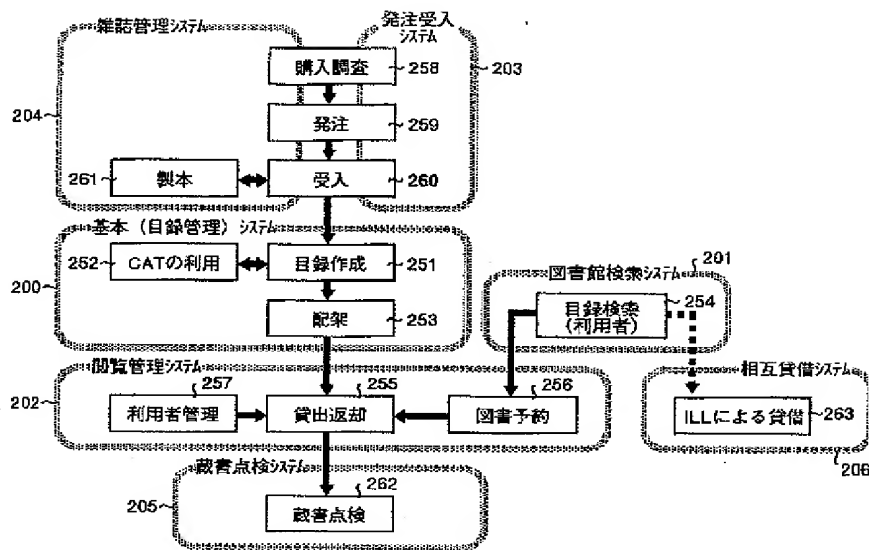
【図 1】



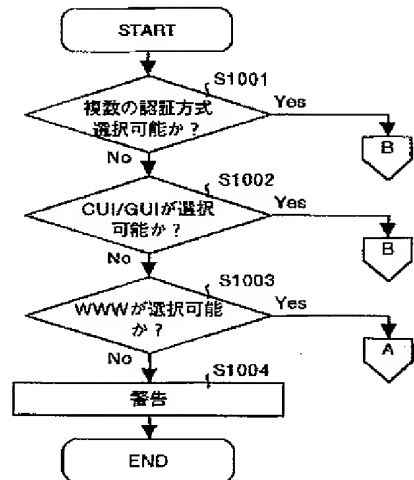
【図 6】



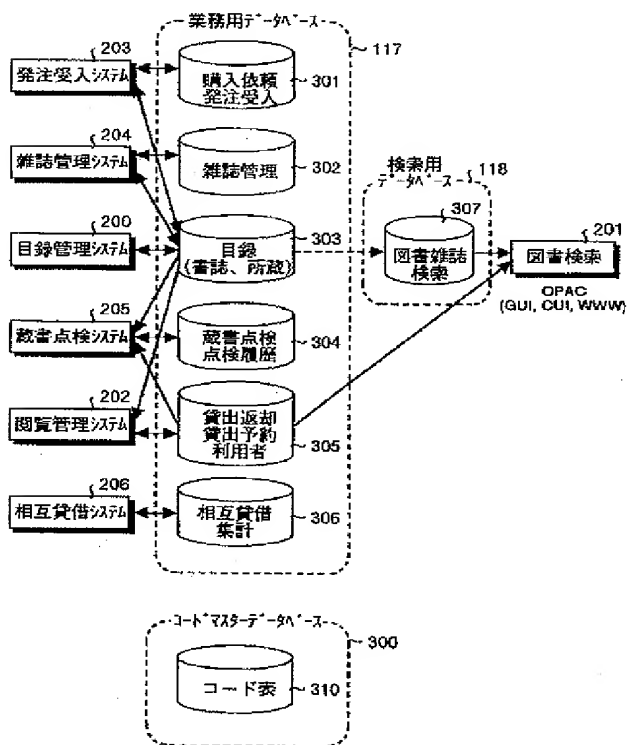
【図 2】



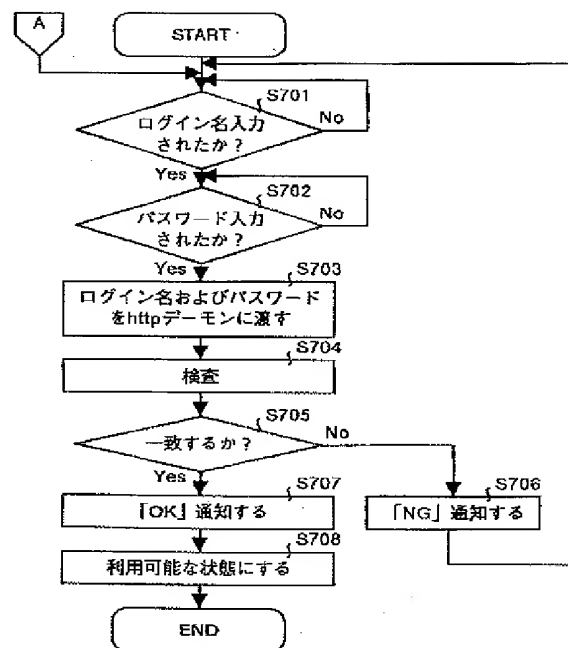
【図 10】



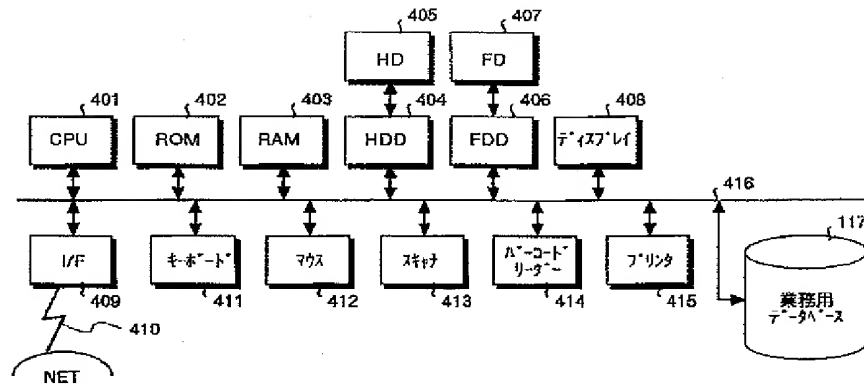
【図 3】



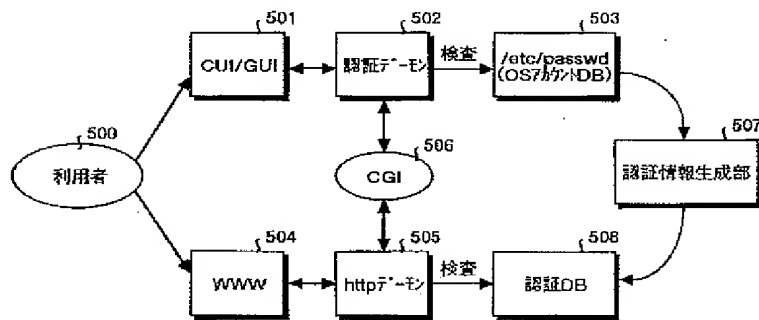
【図 7】



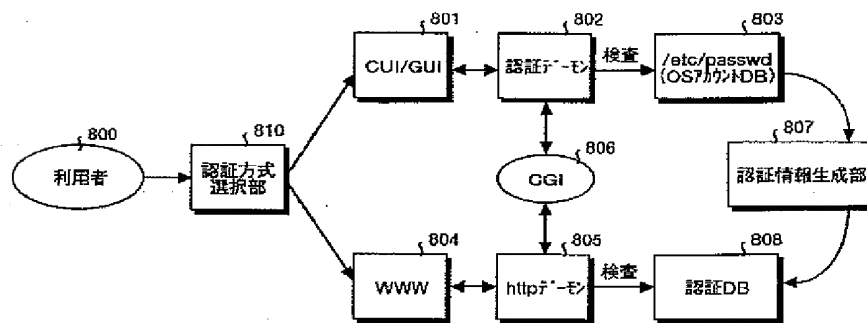
【図 4】



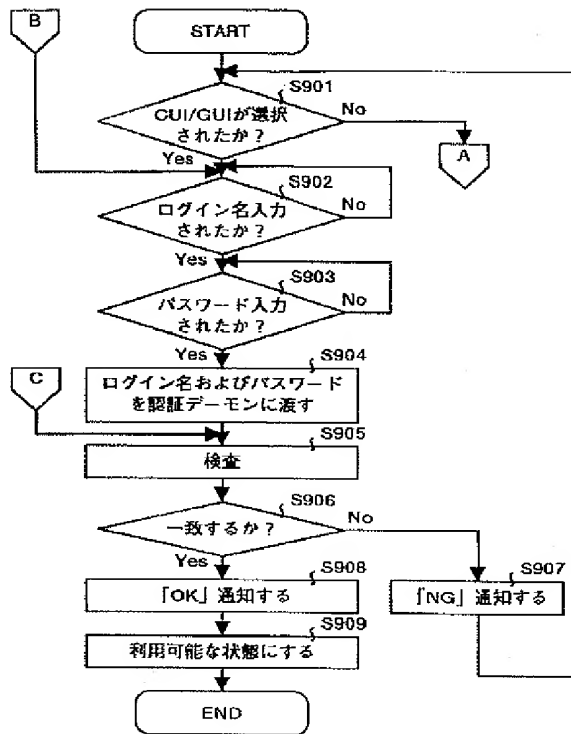
【図 5】



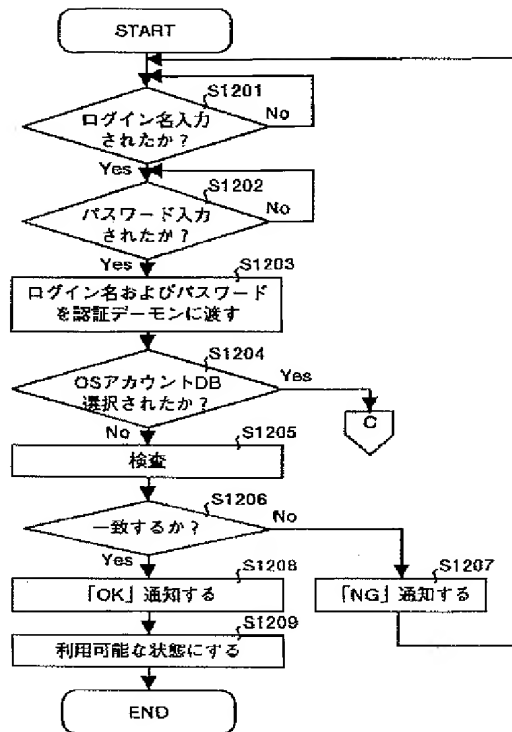
【図 8】



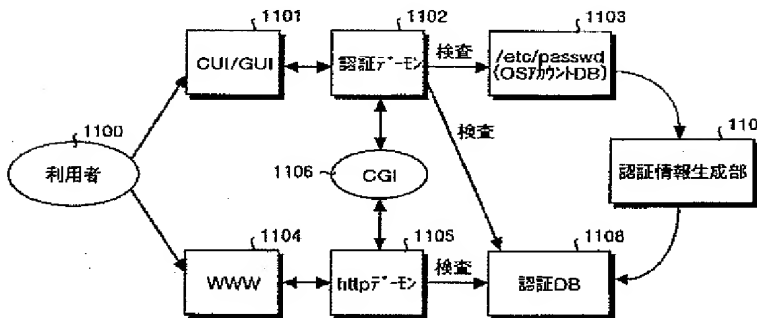
【図9】



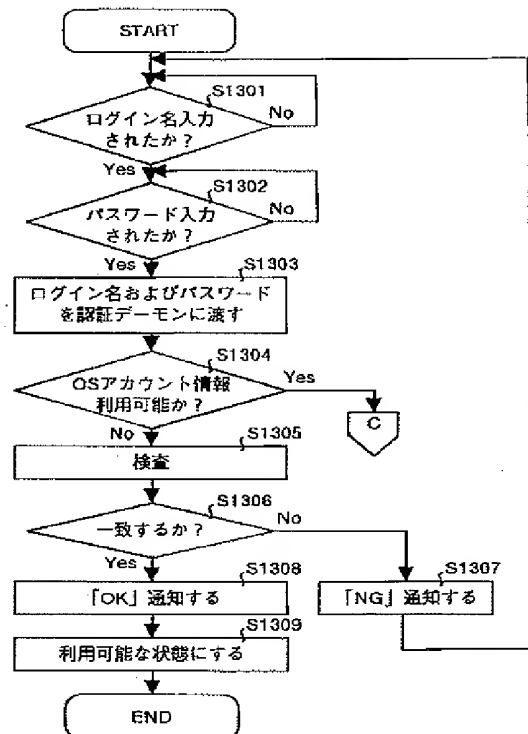
【図12】



【図11】



【図13】



【図 14】

